

REMARKS/ARGUMENTS

By this Amendment, Applicants respond to the Final Office Action dated March 29, 2006 ("Office Action"), in which claims 1, 3, 4, 6-10, 13, 14, 16, 17, 19-23, and 26-28 were rejected. In this Amendment, claims 1, 4, 6, 8, 14, 17, 19, 21, 27, and 28 are amended, and no claims are canceled. After entry of this paper, claims 1, 3, 4, 6-10, 13, 14, 16, 17, 19-23, and 26-28 will be pending in this application.

Rejection of Claims Under 35 U.S.C. § 112

In Paragraph 2 of the Office Action, claims 1, 3, and 4 were rejected under USC §112 as failing to comply with the written description requirement, with particular reference to "local sending client database of security associations" and "receiving client database."

Applicant respectfully submits that the originally-filed disclosure fully supports "local sending client database of security associations." First, at FIG. 13, there is identified a database 1350 that is accessed by a security agent 1310 positioned between a network API 1305 and the network protocol layer 1315. In view of step 1240 at FIG. 12 and page 21, lines 10-12, it is clear that the database 1350 is a "database of security associations." Second, each of the layers 1305, 1310, 1315, and 1320 in FIG. 13 form a common protocol stack on a common nodal entity such as a sending client computer hosting that protocol stack, and being connected to the "network 150" by a single line in the illustration. Finally, the instant specification teaches at page 22, line 21 – page 23, line 2 that "the database of selector/security association pairs is populated by a client when the client accesses key server 140 and receives keying information."

(emphasis added). This provides further support that the database 1350 is local to the client (sending or receiving), because it would make little sense for a client to perform a remote query to a key server, only to again store the results remotely, when the requested data is going to be used locally. Rather, for this portion of the claimed invention, the keying information for several selector/security associations is stored locally in the database 1350, the "local sending client database of security associations," allowing for quick lookup and retrieval to assist in real-time decryption of successive event segments.

It is also respectfully submitted that "receiving client database" is also disclosed in the specification as originally filed. For example, FIGS. 12 and 13 portray both sending clients (operating in a forward or encrypting direction down the protocol stack) and receiving clients (operating in a reverse or decrypting direction up the protocol stack), as evidenced by blocks 1260 and 1270 in FIG. 12, and as evidenced by the bidirectional arrows between protocol stack elements in FIG. 13. In view of FIGS. 12-13 and the accompanying specification text at page 20, line 4 through page 23, line 2, one skilled in the art would readily understand that the database 1350 represents (i) a "sending client database" local to the sending client in the case of outbound traffic going from the network API to the network protocol layer, and (ii) a "receiving client database" at receiving clients in the case of inbound traffic going from the network protocol layer to the network API.

In Paragraph 3 of the Office Action, claims 27 and 28 were rejected under 35 USC §112 as being indefinite, with reference to the term “relatively short.” However, as stated in the MPEP at § 2173.05(b):

The fact that claim language, including terms of degree, may not be precise, does not automatically render the claim indefinite under 35 U.S.C. 112, second paragraph. *Seattle Box Co., v. Industrial Crating & Packing, Inc.*, 731 F.2d 818, 221 USPQ 568 (Fed. Cir. 1984) . . . When a term of degree is present, determine whether a standard is disclosed or whether one of ordinary skill in the art would be apprised of the scope of the claim. MPEP 2173.05(b).

Here, in claims 27 and 28, the term “relatively short” is recited directly in the context of a standard. In particular, the timewise intervals are relatively short “compared to said event duration” (emphasis added). Moreover, there are many examples given in the specification text that would cause the timewise intervals as being understood as “substantially shorter than” or “of generally minor duration” compared to the whole event. Examples are included at page 12 (a 1-hour window as compared to a continuous newscast from a pay television statement) and at FIGS. 6-7 (5 time units as compared to an overall duration greater than 20 time units).

In Paragraph 4 of the Office Action, claims 1, 8, 14, 21, 27, and 28 were rejected under 35 USC §112 as being indefinite, with reference to the term “similar plurality.” It is believed that the inclusion of claims 27 and 28 in Paragraph 4 was a typographical error, because the term “similar plurality” is not contained in claim 27 or 28. In each of the other claims 1, 8, 14, and 21, the term “similar plurality” has been replaced with the term “corresponding plurality,” which is believed to render this issue moot. In particular, the “corresponding plurality of selector/security association pairs” at the “receiving client

database" will now be clearly understood as those that would reverse the security operations performed at the "sending client database" by the "plurality of selector/security association pairs" stored there. Direct support in the instant specification can be found at page 22, lines 12-14.

Rejection of Claims Under 35 U.S.C. § 102(e)

In Paragraph 5 of the Office Action, claims 1, 3, 4, 6-10, 13, 14, 16, 17, 19-23, and 26-28 were again rejected under 35 USC §102 as being anticipated by U.S. 6,289,450 to Pensak, et al. ("Pensak"), the Examiner indicating that Applicant's remarks filed on February 6, 2006 were considered but not deemed persuasive. Applicant earnestly disagrees with Paragraph 5's assertion that Pensak teaches "the receiving client storing a receiving client database comprising a similar [now 'corresponding'] plurality of selector/security association pairs received from the key server." Indeed, this would be plainly contradicted by a prior statement in the Office Action, where it is stated that "Pensak teaches that electronic encryption and decryption keys are not retained by an encrypting or decrypting party." Logically, because one cannot store a database of incoming things that are immediately destroyed prior to receipt of the next incoming thing, the decrypting (receiving) party in Pensak could not possibly store a database of the decryption keys (security associations). The fact that a decryption key in Pensak is destroyed prior to receipt of the next decryption key was explained in the Applicant's remarks filed on February 6, 2006 and, notably, the March 29, 2006 Office Action does not refute this characterization, but instead just repeats the same conclusion. As stated before by Applicant, Pensak teaches an Application Interface 230

at the viewing user's computer 224 that asks the server 206 for the current segment's decryption key (col. 8 line 28), then uses that decryption key to decrypt that segment (col. 8 lines 39-40), and then immediately discards/destroys the key (col. 8 line 41). It is only "when the viewer moves to a different segment" that a subsequent decryption key is requested (see col. 8 line 44).

Moreover, the only additional passage cited by the Office Action in support of its repeated conclusion is Column 9, lines 4-12 of Pensak. However, the database 234 recited in that passage of Pensak is not a "receiving client database comprising a similar [now 'corresponding'] plurality of selector/security association pairs received from the key server," because the database 234 is located at the "remote server 206" itself (*i.e.*, the "key server") which lies across the network from the viewing user's computer 224.

Notwithstanding the above remarks, in an earnest effort to move the present application toward prompt allowance and issue, the following additional limitation has been added to each of the independent claims:

"wherein, for any particular one of said timewise intervals of said event having a corresponding selector/security association pair, the receiving client receives said corresponding selector/security association pair from said key server and stores said corresponding selector/security association pair in said receiving client database prior to receiving said particular one of said timewise intervals of said event" (see claims 1, 6, 14, 19, 27, and 28).

Thus, as amended, each independent claim 1, 6, 14, 19, 27, and 28 clearly specifies that the receiving client receives the decryption key prior to receiving the segment to be decrypted by that key, *i.e.*, "prior to receiving said particular one of said

timewise intervals of said event.” This is contrast to Pensak, in which the viewing user’s computer 224 only opens the Configuration Utility 226, the Administrator Utility 228, and the Application Interface 230 after recognizing that the segment is encrypted (col. 8, lines 4-6), and the decrypting key is not delivered until after those programs request such key from the remote server.

At a more general level, the above-identified differences between Pensak and the present invention as recited in 1, 6, 14, 19, 27, and 28 are logically consistent with the differences in the overall purposes of the disclosures. The presently claimed invention is directed primarily to security operations consistent with immediate, real-time display of successive program segments, whereas Pensak is directed -- notwithstanding some brief genericizing language at col. 3, line 4 -- toward security operations for documents such as PDF files, where real-time immediacy is not an issue. Thus, because of the substantial differences between Pensak and claims 1, 6, 14, 19, 27, and 28, and in view of the substantially different technical goals toward which each is directed, it is respectfully submitted that none of claims 1, 6, 14, 19, 27, and 28 is anticipated or suggested by Pensak.

CONCLUSION

In view of the foregoing amendments and remarks, Applicants submit that the pending claims are in allowable form, and respectfully request reconsideration of the rejections and timely allowance of the pending claims.

Appln. No. 09/544,493
Amendment Dated August 24, 2006
Reply to Final Office Action Dated March 29, 2006

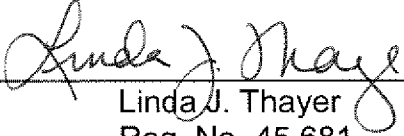
PATENT
Customer No. 22,852
Attorney Docket No. 07451.0033-00
Intertrust Ref. No. IT-47 (US)

Please grant any extensions of time required to enter this response and charge
any additional required fees to our Deposit Account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: August 24, 2006

By: 
Linda J. Thayer
Reg. No. 45,681

Finnegan Henderson Farabow
Garrett & Dunner L.L.P.
901 New York Ave., N.W.
Washington, D.C. 20001
Attorney direct (650) 849-6621